APPLYING IDENTIFY MANAGEMENT AND CRYPTOGRAPHY TO ICS

Jack Krohmer
Vern Williams
Ralph Poore

Agenda

SCADA Security History:
From Nothing To Not Enough
Jack Krohmer
Industrial Controls Engineer

Identity Management:
Linking Identity to Actions
Vern Williams
CISSP, CSSLP, PMP, ISSEP, CBCP

Cryptography using FPGA
Ralph Spencer Poore
CISSP, CFE, CISA, CHS-III, CTGA, QSA

SCADA SECURITY HISTORY: FROM NOTHING TO NOT ENOUGH

Jack L. Krohmer
Process Networks Plus, Inc.

Speaker Biography

- Over 35 years of ICS experience including greenfield start ups and upgrade /renovation of existing facilities.
- Project manager for developing proprietary control system utilizing the Fourth programming language for the operator interface and high level analog controls and Modicon PLC's for discrete control.
- Founded Started Systems Plus in 1985 and incorporated Process Networks Plus, Inc. in 1996.
- Installed one of the first Hybrid DCS systems in 1995 for the ancillary systems of a 450 Megawatt coal fired power plant Programmed using auto cad developed SAMA drawings Compiled and loaded into Modicon controllers.
- Installed a hybrid DCS on a 450 Megawatt power plant in 2000 controlling everything but the Turbine control.
- Currently install Hybrid DCS SCADA systems for Power Generation, Chemical, Mineral Processing and food and beverage industries.

History of SCADA Security

- SCADA traditional security focus
  - Design systems with good physical security
  - Design resistance to operator error
- Networked control system access
  - Added enough security to make sure we had control of who could access what from where to prevent operator error not to keep the bad guys out
- Business to Control System Interconnects
  - Customer desire to connect our control networks to their business networks were initially rejected as bad engineering practice.
  - With the advent of modern network routers and managed switches resistance was futile as businesses allowed access to control networks, but now with adequate controls

History of SCADA Security

- Communication or identity security was not available in controllers until some time after 2000.
- Control system integrators face customer resistance to any security measures due to:
  - Concerns about operator inability to act during critical control actions due to login failure
  - Delays due to security exceeding critical control loop timing
- Some System Operators that are most vulnerable rely on physical security and group policies to provide security
- It has been obvious to me for some years that our systems, especially in critical infrastructure facilities such as power generation and distribution are very vulnerable because of inadequate security and that sooner than later these systems will be compromised and disrupted.

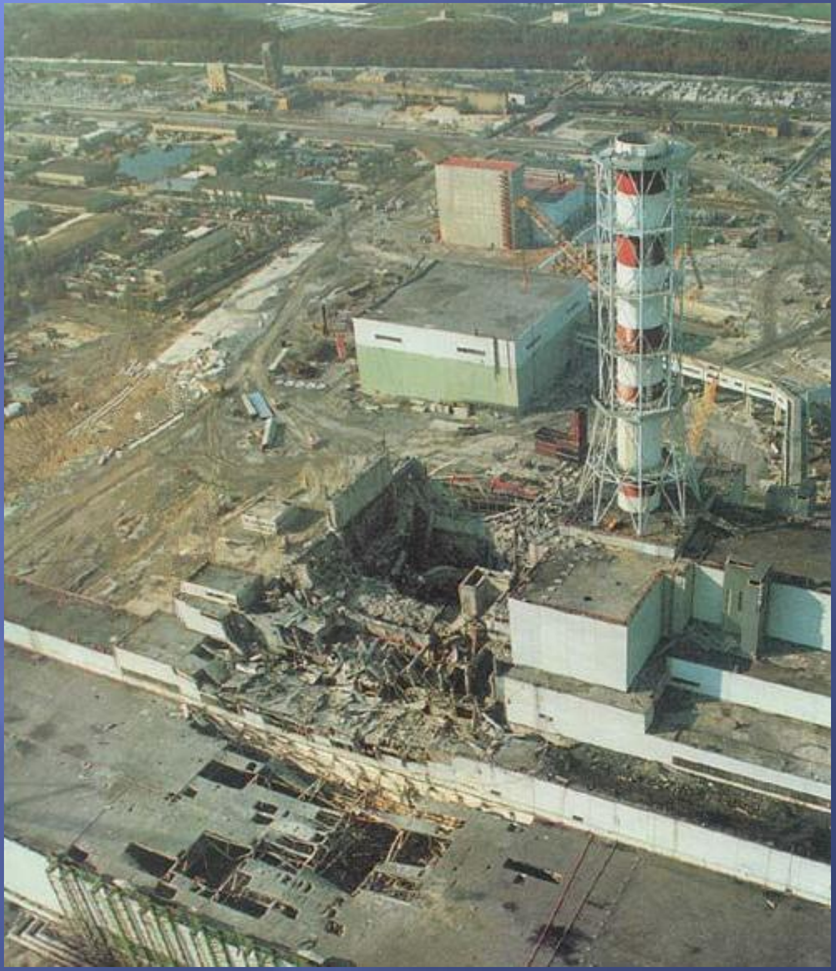
Its Later Than You Think!!!

- CONFICKER & STUXNET WORMS HAVE BROUGHT THE FUTURE TO US SOONER THAN EXPECTED!
- Conficker – we have a good idea where it came from and how it spreads but the contents are so well encrypted that we don't know what it is programmed to do.
- Stuxnet Compromise at Iranian Nuclear Plant May Be By Design By USA and Allies
- Stuxnet designed to infiltrate heavy–duty industrial control systems

Its Later Than You Think!!!

- **Conficker & Stuxnet worms have ushered in a dangerous future sooner than expected!**
- Conficker:
  - Know where it came from and how it spreads but due to encryption the ultimate purpose is still a mystery
- Stuxnet:
  - Compromise seems targeted at the Iranian Nuclear Plant and may be designed by US or Allies
  - Robust Malware designed to infiltrate heavy-duty industrial control systems

Stuxnet and its descendants could cause a repeat of Chernobyl, April 26, 1986



LINKING IDENTITY TO ACTIONS

Vern Williams, CISSP CSSLP PMP ISSEP CBCP
Computer Security and Consulting Services, LLC
President & Security Architect
ISSA and IEEE Senior Member

Speaker Biography

- Nuclear Submarine Officer in the US Navy for 20 years
- Masters of Science in Information Systems
- Over 20 years of information technology and security engineering and architecture experience
- Instructor for (ISC)^2 Certified Secure Software Lifecycle Professional
- Director of Operations for ISSA International 2007-9
- Senior Member of ISSA and IEEE

Linking Identity to Actions

- Robust IdM: no longer optional
- Identity Proofing
- Applicable Technologies
- Robust Identity Management

- Follow on to ICSJWG Spring Conference Session
  - The Silent Risk We are Living With: INSIDER THREAT
  - Pan Kamal, CISAAlertEnterprise, Inc.

Available Resources

- People
  - Encourage: do right thing when no one is looking
  - Lead: solve todays problems
  - Inspire: to become tomorrows leaders
- Processes
  - Document: enable continuity
  - Measure: metrics with a purpose
  - Improve: do one thing you can do
- Products
  - Start with a plan (Architecture)
  - Look beyond your current comfort zone
  - Implement as a project

Protection Candidates

- Hosts
- Network Infrastructure
- Applications
- Data

Implement secure images and practices, establish a baseline and control configurations and changes to all of the above.

Robust IdM: no longer optional

- Passwords are Insecure and Easily Broken
- Access control, the heart of security, is :
  - Allowing only authorized users, programs, or processes access to systems or resources;
  - Granting or denying, according to a particular security model, permission to access a resource;
  - Set of procedures--performed by hardware, software, and administrators--to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules
- Multifactor Authentication is key for critical systems or elevated privileges.

Identity Proofing

- Identity Proofing –The process by which the credential issuer validates sufficient information to uniquely identify a person applying for the credential. (NIST)
  - Prove that the identity exists
  - Prove the applicant is entitled to that identity
  - Address the potential for fraudulent issuance of credentials based on collusion
- Identity Source Documents: Need 2 I-9 Identity Sources
  - Must include a government-issued picture ID and fingerprints (10 for identification and two for verification)
- Background Checks: SF 85
  - Required Investigations based on the information provided in SF 85 and the Identity Source Documents

Applicable Technologies

- Biometrics
  - Facial Recognition
  - Dynamic Signature
  - Fingerprint Recognition
  - Hand Geometry
  - Iris Recognition
  - Palm Print Recognition
  - Speech Recognition
  - Vascular Pattern Recognition
- Automated Identity Proofing
  - Classic knowledge-based authentication (KBA)
  - Dynamic KBA
  - Out-of-band proofing

Robust Identity Management

- Thorough Identity Proofing
- Granular Role Based Access Control (RBAC)
- Multi-Factor Biometric / Certificate Authentication
- Graceful failure modes
- “Break Glass” with alerting and logging

Resources

- PIV Program (see also FIPS 201 and NIST 800-73, 76, 78, 85, 96, 104, 116)
  - http://csrc.nist.gov/groups/SNS/piv
- FIPS 201.com
  - www.fips102.com
- Biometrics Catalog
  - http://www.biometricscatalog.org
- Biometric Consortium
  - http://www.biometrics.org/

CRYPTOGRAPHY USING FPGA

Ralph Spencer Poore, CISSP, CFE, CISA, CHS-III, CTGA, QSA
Cryptographic Assurance Services LLC
President & Chief Cryptologist
(ISC)^2 Advisory Board of the Americas

Speaker Biography

- Over 30 years of information technology experience with emphasis on privacy, security, audit, and control in electronic commerce, enterprise systems and enabling technologies
- Security executive positions at Ernst & Young, Coopers & Lybrand, Innové, Caremark, Privacy Infrastructure, Inc. and Cryptographic Assurance Services, LLC.
- $(ISC)^2$ Advisory Board of the Americas member and co-chair of the Executive Writers' Bureau
- Associate Editor for the $(ISC)^2$ Journal
- Inventor (with patents), author, speaker, and applied cryptographer

Overview

- Advantages of hardware-based cryptography
- Field-Programmable Gate Array (FPGA)
- Cryptographic design issues with FPGA
- Application to Identity Management

Hardware-based Cryptography

- Ability to make tamper-resistant (e.g., FIPS 140-2, Level 3+)
- Speed
- Meet special needs of small size, environment, power consumption, etc.

FPGA

- Advantages of FPGA
- Risk of FPGA
- Alternatives

Cryptographic Issues

- Mechanisms for high reliability
- Programming integrity
- Zeroization
- Device authentication
- Key management

Application to Identity Management

- At manufacture
- Once fielded
- Importance of registration process

Questions ?

Contact Information

- Jack Krohmer
  - President, Process Networks Plus
  - 512-533-3752
  - JLKrohmer@pnplus.com
- Vern Williams
  - President and Security Architect, Computer Security and Consulting Services, LLC
  - 512-297-8798
  - Vern.Williams@IEEE.org
- Ralph Spencer Poore
  - President & Chief Cryptologist, Cryptographic Assurance Services LLC
  - 817-235-8472
  - Ralph.Poore@cryptographicassuranceservices.com